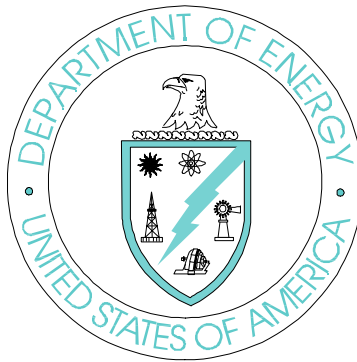


Considerations for Implementing Digital Signatures

**at the
U. S. Department of Energy**



June 16, 1998

**Assistant Secretary for Human Resources and Administration
Deputy Assistant Secretary for Information Management**

Foreword

Digital signature technology is still quite new, and many issues have been identified for more in-depth examination. This initial issuance of *Considerations for Implementing Digital Signatures at the Department of Energy* provides an overview of the technology as initial guidance for implementation at DOE. The document provides questions to be answered and issues to be addressed in future updates. As such, it provides an introduction to describing the steps necessary to: develop, implement, and maintain a reliable means of secure electronic messaging (when text is also encrypted) over open, unsecured computer networks; minimize or eliminate the incidence of forged digital signatures and possible fraud in electronic transactions; and establish standards and procedures for verification and reliability of electronic transactions. Because the digital signature environment is dynamic, it is important to develop guidelines that will promote interoperability.

This document is intended for both technical and nontechnical audiences. It should be helpful to anyone contemplating the implementation of digital signature for any application. Program managers, legal staff, records managers, software support staff, and security specialists should all benefit from understanding these considerations. It should be of particular interest to staff involved in setting up Public Key Infrastructures.

The following aspects of implementing digital signatures are discussed.

- **Public Key Infrastructure**—Third parties may perform the service of verifying and certifying the association between a digital signature and a particular person or entity. Such a third party may also serve as a repository for these certificates. This third party is known as a certification authority.
- **Digital Signature Applications**—Digital signatures can be used for e-mail, electronic funds transfer, electronic data interchange, software distribution, data storage (to provide verification of integrity of data at a future time), and other applications that require data integrity assurance and data origin authentication.
- **Digital Signature Standards**—The standards presented in this document are already part of the DOE profile of adopted IT standards. These standards represent guidance for achieving interoperability Departmentwide, Governmentwide, and with the private sector.
- **Records Management**—Usually records management concerns are not particularly considered when implementing new technology. However, with digital signature implementations, it becomes important to include records managers in the planning stages.

- **Legal Considerations**—The formal requirements for legal transactions, including the need for signatures, vary in different legal systems and with the passage of time. Implementing requirements for creating and verifying a digital signature accomplishes the essential elements needed for legal purposes.

The Digital Signature Working Group (DISIWG), founded in July 1996, is made up of DOE staff, both Federal and contractor, who are investigating and implementing the technology at their sites. DISIWG enables the DOE community interested in the implementation of interoperable, cost-effective digital signature applications to work together to identify corporate issues, to identify partnership opportunities and to share information about digital signature and public key infrastructure activities. DISIWG meets once a month via teleconferencing to discuss issues of mutual concern. Working group members served in subgroups to write portions of this document. Current participants include:

- Albuquerque Operations Office
- Allied Signal - Kansas City
- Brookhaven National Laboratory
- Continuous Electron Beam Accelerator Facility
- Chief Financial Officer
- Chief Information Officer
- General Counsel
- Chicago Operations Office
- Argonne National Laboratory
- Lawrence Berkeley Laboratory
- Lawrence Livermore National Laboratory
- Nevada Operations Office
- Oakland Operations Office
- Oak Ridge Operations Office
- Office of Scientific and Technical Information
- Sandia National Laboratories
- Savannah River Operations Office
- Waste Isolation Pilot Project
- West Valley Field Office

Participation in DISIWG is open to all DOE elements, both Federal and contractor. For more information, please contact the meeting chairman: Phil Sibert, Phil.Sibert@hq.doe.gov, 301-903-4880.

The graphics appearing throughout the document were furnished by John Vollmer of Argonne National Laboratory. Reference materials used in preparing the document appear in the Appendix.

Table of Contents

Foreword	ii
Chapter 1 Digital Signature Overview	1
Chapter 2 Public Key Infrastructure	5
Chapter 3 Digital Signature Applications	8
Chapter 4 Digital Signature Standards	14
Chapter 5 Records Management	21
Chapter 6 Legal Considerations	26
Chapter 7 Next Steps	31
Appendix A: References	

Chapter 1. Digital Signature Overview

What Is a Digital Signature?

With the ever-increasing use of electronic technology, it is necessary to establish a framework for authenticating computer-based information. Electronic messages are rapidly replacing paper in today's environment. These messages are migrating beyond private, limited-function communications to open networks, such as the Internet, with unlimited uses. Because open networks lack rigorous access and usage controls, they are basically unsecure. Consequently, electronic messages are particularly susceptible to altering, tampering, or forging. Digital signatures are a technological answer to these problems.

Digital signatures are key to the viability of electronic commerce, both from a commercial and a legal standpoint. Business information exchanged and activities performed must have the same level of authentication as that of paper-based exchanges and activities that are legally enforceable. Digital signatures are one way to accomplish this.

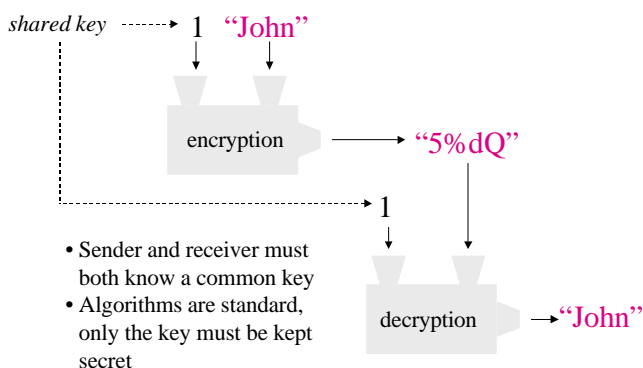
A digital signature is not a pen-and-ink signature nor is it a handwritten signature scanned into a computer and attached to an electronic message. A digital signature is the result of a two-step process that is performed on the message by encryption software that has been loaded onto the sender's computer. Although a digital signature is not handwritten, the process of creating a digital signature and verifying it provides electronically the same effect that a handwritten signature on paper provides. A digital signature enables users to determine who sent a document, identify what document was sent, and determine whether the document was altered in route. It reasonably ensures the recipient that the message came from an identifiable sender and contains a specific, unaltered message. It may be used where sufficient confidence in the source, content, and integrity of a transaction is necessary. A digital signature ensures that a message is authentic, its integrity has not been compromised, and the sender cannot disavow or repudiate the message after sending it.

For a digital signature to work effectively, three obstacles must be overcome. First, a recipient must be able to associate reliably with the sender the private and public key pair used to encrypt and decrypt the message digest. Unlike a pen-and-ink signature, a public-private key pair has no intrinsic association with a particular person. The keys are just large numbers. Second, a recipient needs a trustworthy source from which to obtain the public key needed to verify the message. Third, a digital signature must have the same legal effect as a handwritten signature on a paper document.

Description of Digital Signature Cryptography

Digital signatures are created and verified by cryptography, which transforms messages into unintelligible forms and back again. Digital signatures employ public key cryptography, which uses an algorithm with two different, but mathematically related keys: one key is for creating a digital signature or transforming the data into an unintelligible form; the other key is for verifying a digital signature or returning the message to its original form.

Private Key Mechanics

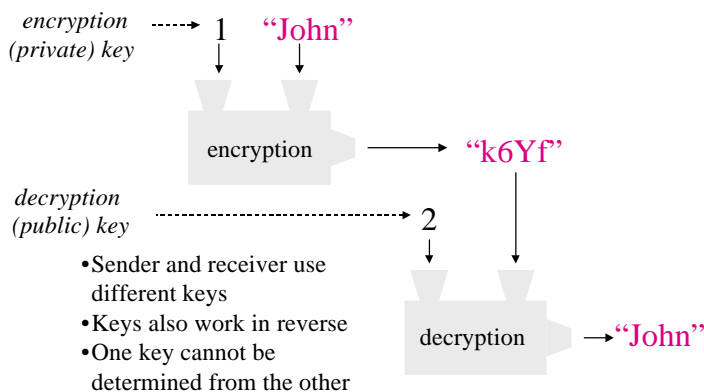


The complementary keys for digital signatures are termed the private key (known only to the signer and used to create the digital signature) and the public key (more widely known and used by a relaying party to verify the digital signature). A public key can be available to anyone needing to verify the signer's digital signature. The public key can reside in an online repository or directory where it is easily accessible. Although the two keys are mathematically related, it is not

computationally feasible to derive the private key from knowledge of the public key. Although many people may know a signer's public key and use it to verify the signer's signature, they cannot discover the signer's private key and use it to forge a digital signature.

Another process called a hash function is used in creating and verifying a digital signature. A hash function is an algorithm that creates a digital representation or fingerprint in the form of a hash value of a standard length that is usually smaller than the message, but unique. Any change to the message produces a different hash result when the same hash function is used. Hash functions enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content. Therefore, hash functions efficiently provide assurance that there has been no modification of the message since it was digitally signed.

Public/Private Key Mechanics

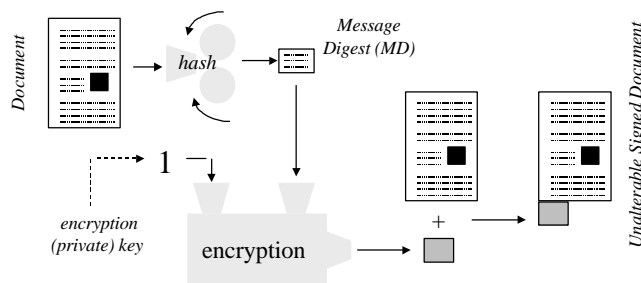


Typically a digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. However, it may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital signature is unique to its message, it is useless if disassociated from its message.

The Digital Signature Process

How Does Public/Private Key Provide a Signature ?

- A message digest is appended to the document



The digital signature process assumes two users have agreed upon a hash function and a signature algorithm for the signature verification process. An originator who needs to send a signed message performs the following:

- Generates a digest for the message
- Computes a digital signature as a function of the digest and the originator's private key
- Transmits the message and signature to the recipient.

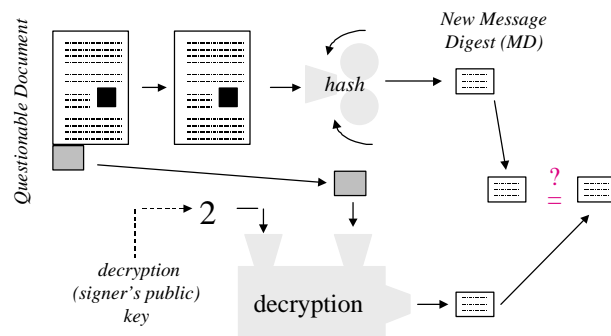
Upon receiving the message, the recipient performs the following procedure.

- Generates a digest for the message received
- Uses the digest, the originator's public key, and the signature received as input to a signature verification process.

If the signature is verified, the recipient is assured that the message was not modified and that the originator sent the message. If any portion of the original message was changed, the digest generated using the received message causes the signature verification process to fail.

How Does Public/Private Key Provide Authentication?

- The message digest can be later validated



Benefits of Digital Signatures

Digital signatures, if properly implemented and used, offer solutions for the following.

- **Impostors**—Minimizes the risk of dealing with impostors or people who try to deny responsibility by claiming to have been impersonated
- **Message Integrity**—Minimizes the risk of undetected message tampering and forgery and the claim that a message was altered after it was sent
- **Formal Legal Requirements**—Strengthens the view that legal requirements, such as writing, signature, and original document, are satisfied since digital signatures are more valid than paper forms
- **Open Systems**—Retains a high degree of information security, even for information sent over open, unsecure, but widely used, channels.

Business Case

When making a business case for using digital signature, an important consideration is whether a digital signature is really needed as opposed to a simple electronic approval. In many cases, signatures are affixed to paper documents because it is an expedient and easily available way to do business, not because a legally binding, unalterable signature is needed.

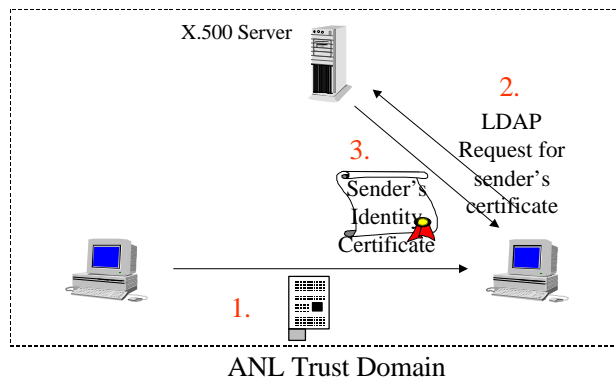
When reengineering a work process, in addition to making it paperless, it is important to analyze whether a signature is really a necessary part of the process. At least for pilot implementation of digital signature, where there will be a high overhead and steep learning curve, it will be important to choose applications that truly require authentication/non-repudiation.

Chapter 2. Public Key Infrastructure

In order to verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. In transactions involving only two parties, each party can simply communicate the public key of the key pair each party will use. As electronic commerce moves to the Internet where significant transactions occur, the problem of authentication/nonrepudiation becomes one of efficiency and reliability. A Public Key Infrastructure (PKI) provides the means to bind public keys to their owners and helps in distributing reliable public keys in large heterogeneous networks. PKI allows persons without prior knowledge of each other to engage in verifiable transactions.

So, where do I get somebody's public key?

•Ans: You ask our X.500 server for a copy of their certificate



PKI uses one or more trusted third parties to associate an identified signer with a specific public key. That trusted third party is referred to as a certificate authority (CA). CAs issue a digital certificate that identifies the CA issuing it, identifies the subscriber, contains the subscriber's public key, and is digitally signed with the CA's private key. To obtain a digital certificate, the subscriber who wants to digitally sign a message or document presents a copy of his public key along with sufficient proof of identity to the CA. Once satisfied as to the identity of the

subscriber, the CA issues the subscriber a digital certificate. To make a public key and its identification with a specific signer available for use in verification, the certificate is published in a repository or directory. Certificates can be automatically retrieved by having the verification program directly access the repository.

When the subscriber wants to use the digital signature, he transmits a copy of his digital certificate to the recipient of his digitally signed message. Upon receipt of the signed message, the recipient's computer confirms with the CA identified in the digital certificate that the sender is who he purports to be and that his certificate has not expired or been revoked. All of this activity is transparent to the recipient.

Certificate authorities certify public keys, create and distribute certificates, and generate and distribute certification revocation lists, which are posted on a designated repository or directory.

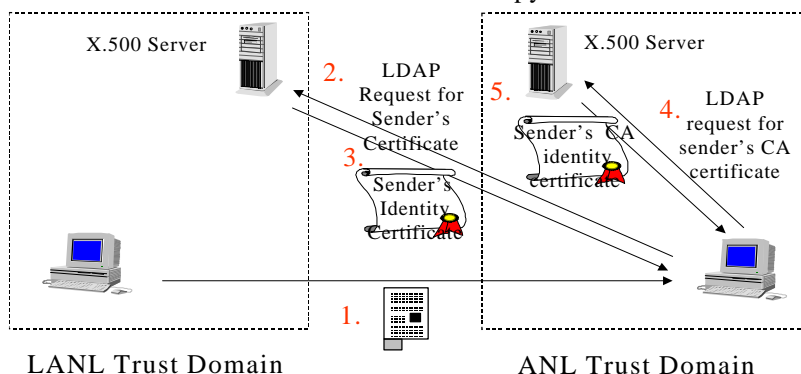
A certification revocation list contains the serial number of certificates that have been reported by their owners as having been compromised.

A certificate infrastructure provides a uniform way to obtain certificates in spite of the possible differences in certificate management policies used by different segments of the infrastructure. In addition, mechanisms are provided to enable each user to be aware of the policies governing any certificate encountered.

So, where do I get somebody else's public key?

With a certificate authority infrastructure in place, a relying party can be reasonably assured that the document is what it purports to be and that the signer is a particular person. There will be institutional overhead associated with establishing and utilizing certification authorities and repositories, and there will be costs to signers and relying parties. On the other hand, problems associated with imposters, message integrity, and formal legal requirements can be resolved.

•Ans: You ask their X.500 server for a copy of their certificate



It is necessary to consider the integrity and security of the PKI components. The confidence that can be placed in the binding between a public key and its owner depends on the confidence that can be placed on the system that issued the certificate that binds them. Provisions in the X.509 standard (addressed in Chapter 4, Digital Signature Standards) enable identification of policies that indicate the strength of mechanisms used and the accepted standards of certificate handling. By examining the policy associated with a sender's certificate, the recipient of a signed or encrypted message can determine whether the binding between the sender and the sender's key is acceptable and thus accept or reject the message.

The Department of Energy has developed Chapter 9 of the Telecommunications Security Manual, DOE M 200.1-1, which "defines the roles, requirements, and responsibilities for establishing and maintaining the documentation necessary to ensure that all certificates are managed in a manner that maintains the overall trust required to support a viable PKI."

Chapter 9 applies to all certification authorities or certification authorizations on behalf of DOE and requires the development of certificate policy documents and certification statements that are approved by the DOE Policy Management Authority. The certification authorities that apply perform the following functions.

- Participate in cross-certifying with DOE PKI operated by DOE Policy Management Authority
- Issue certificates used to process or protect Unclassified Controlled Nuclear Information (UCNI), Official Use Only (OUO), and other Federal, sensitive, unclassified information that requires encryption
- Issue certificates for the following purposes:
 - S** To establish financial obligations for, or on behalf of, the Federal Government
 - S** To establish or verify identity of recipient of information when authority to receive such information is already established
 - S** To establish or verify identity of recipient to access classified computing resources when authority is already established.

The chapter sets forth requirements for DOE elements that have implemented or plan to implement public key systems. The requirements shall be used to establish minimum DOE operational policies and procedures to assess CA operations. Chapter 9 also addresses establishing an organizational structure and defines responsibilities of the CAs, registration authorities, etc.

Chapter 3. Digital Signature Applications

Uses of digital signature are endless. Some of the potential uses at DOE are:

- Electronic commerce
- Fully integrated electronic support of work processes such as travel
- Official personnel documentation—W-4 forms, time cards, personnel actions
- Secure unclassified communications where end-to-end authentication and non-disclosure are required—faxes, e-mail, video conferencing, remote log-in
- Technical drawings and other images—protection of access to research data (drawings), time-stamping procedures for proof of patent, disclosure protection of drawings in transit and storage. (Drawings associated with weapons data would be included in this category.)
- Virus detection before a program is executed, since even a minute change is detected
- Authentication and access control to web pages and web forms
- Electronic laboratory notebooks as legal records for patent considerations. (This involves the issues of date and time stamping of the contents of the electronic notebook and verification that the contents of the electronic notebook are a complete and unaltered record. This must all be done in a fashion that is verifiable and acceptable to the courts before widespread utilization of the electronic notebook.)
- Contracting—Ensuring that contract agreements that have occurred in an electronic (non-face-to-face environment) are enforceable, implementing contract bidding and formation on a large scale without the individual bid issuers having to establish a personal trust relationship with the organizations/contractors in question.
- Information transfer or publication—Issuing "official" web pages through the use of well-known public keys, vouched for by Internet-trusted third parties. (The previously unintroduced parties are the web-site and end-users such as reporters, investors, etc.)
- Sharing R&D and technology transfer information with universities and scientists world wide

- Authorizing remotely operated experiments
- Acting as a software bus for exchanging information between applications

A number of vendors are offering CA services and products to support electronic commerce and user authentication applications within an enterprise. These entities include, but are not limited to:

- VeriSign
- GTE CyberTrust/BBN
- Entrust Technologies
- IBM World Registry
- TradeWave
- CertCo LLC
- Xcert Software
- United States Postal Service (USPS)/Cylink
- Netscape Communications
- Microsoft

Following is a discussion of these products and services.

VeriSign

VeriSign is the only independent company focused on certification for corporations and consumers. The company was founded as a spinoff of RSA Data Security. VeriSign has done the most to educate the market about digital certificates, which it prefers to call digital IDs. It has issued nearly 1 million certificates, including 25,000 secure server IDs. In July 1997, VeriSign announced an alternative service to certificate servers, VeriSign OnSite. VeriSign OnSite lets companies set up an in-house CA to secure communication and information exchange over corporate TCP/IP networks. Enterprises using VeriSign OnSite can provide secure e-mail (using S/MIME) and intranet access to their proprietary corporate information. The product is designed as a quick-to-deploy, easy-to-manage intracompany digital ID program offered at lower cost and less effort than “do-it-yourself” certificate servers because it leverages VeriSign’s back-end infrastructure.

GTE CyberTrust/BBN

The GTE CA unit, called CyberTrust, is part of the GTE Network Systems Division, a commercial division that was spun off from a government services unit that offered security services to U.S. government agencies and the military. The organization provided very large public key certification and key management systems that have been operational for more than ten years. Much of that activity was related to confidential telephone communications (third generation secure terminal unit key management), and for secure X.400 messaging. The CyberTrust Customer-Branded Service is an outsourcing approach with GTE providing back office operations. The CA product allows entities to be their own CAs. Customers can start with an outsourced service and migrate to their own system.

In April 1997, GTE announced plans to acquire BBN. BBN was targeting the high-end market with a certificate issuing product, called SafeKeyper certificate management system (CMS), which offers flexible features and promises scalability for use in large certificate-using applications. The primary target markets are financial institutions wanting to offer direct access to accounting or marketing information using browsers over the Web. The typical infrastructure targeted is one planning to issue 100,000 to millions of certificates to customers or remote users who access sensitive information.

Entrust Technologies

In January 1997, Northern Telecom Ltd. (Nortel) announced the formation of Entrust Technologies. Before the spinoff, Nortel Secure Networks, a business unit, managed the Entrust product family. Entrust is the leading vendor in providing enterprise-based CA products. In addition to issuing certificates, Entrust addresses the more difficult task of managing key life cycles. Entrust has entered an impressive array of partnerships with vendors that have made their products "Entrust-ready" or that are marketing products and services based on Entrust. Entrust's strengths lie in its ability to provide an end-to-end solution, embracing several elements of security, while remaining vendor neutral.

IBM World Registry

IBM plans to offer a certification product and a CA service. The product and service are based on the Entrust Technologies' certificate authority engine. The product, called Registry, and the service, called World Registry, provide a Web-based PKI that uses digital certificates to authenticate the parties involved in a transaction. The Registry is designed for in-house operation. Applications are built on a secure Web server that uses Australian telecommunication company Telstra's View500 directory to store certificates. IBM's enhancements include a key ring manager that handles multiple certified keys on browsers, PC cards, smart cards, and other media.

TradeWave

Operating a CA based on Entrust's approach and with the involvement of IBM's World Registry service, TradeWave is operating the Open Access Same-time Information System (OASIS) project for deregulated utilities to sell power on an open market. The buyers, including municipalities and other large power users, are committing themselves to millions of dollars of electricity; accordingly, certification of users is a requirement for this application.

CertCo LLC

Banker's Trust has spun off its internal unit, CertCo, which aims to enable trusted third parties to become CAs. CertCo launched its products in 1997. Besides providing certification services, CertCo is developing technology to enable trust institutions to do business on the Internet. The spinoff combines expertise in cryptography, risk management, law, technology and banking processes and procedures to target primarily the business-to-business market for secure electronic commerce applications. CertCo will work through partners, primarily banks and other financial institutions to license its technology and business practices and to offer the institution's customers certification and other services.

Xcert

Xcert was formed in April 1996 by individuals involved with Nortel and Microsoft to develop public key applications. While offering Sentry CA, a CA server, Xcert's core technology product and differentiator is its XUDA (Xcert Universal Database) programmers interface technology, a secure sockets layer-secured, lightweight directory access protocol-compliant toolkit for developers, used for accessing distributed, multiplatform encryption modules. The technology behind the product is a database back end tuned for transactional environments and based originally on X.500 directories. XUDA supports access to multiple, distributed databases, allowing multiple public key infrastructures to exist on a cross platform basis. The application programming interface (API) is cryptographically independent—it uses any cryptographic module.

U.S. Postal Service/Cylink

The USPS proposed digital ID certificate program appears directed primarily toward applications such as citizen relationships with government agencies including the Internal Revenue Service, Department of Motor Vehicles, and social benefit programs. Potential uses are within and among Government agencies. For example, USPS has been working with the Federal Aviation Administration on a document certification project. The CA capability is part of the USPS Electronic Commerce System, a set of initiatives designed to maintain the relevance of the service and provide new revenue sources in an era of electronic messaging.

The plan for the USPS certification process is for customers to present positive identification and their public keys to the USPS officials who, in turn, will digitally sign those keys and issue a diskette or smart card containing the certificate. Several versions of certificates will be offered. A basic certificate will not require proof of identity. A certified certificate would require similar identification proofs as does a passport. Eventually, the USPS will issue tokens to consumers, likely using biometrics such as thumb prints to bind a public key and a user. The estimated cost to consumers of receiving and maintaining a certificate is \$15-20 per year. Cylink is contracting with the USPS to design and implement the CA. Further, Cylink has announced CA capabilities for its network management products.

Microsoft

As part of its Internet Security Framework, in June 1996, Microsoft announced a series of planned initiatives related to CA and PKI. For example, CryptoAPI version 2.0 provides a public key infrastructure, including certificate-based authentication services and extensible certificate management functions. Microsoft's Certificate Server issues, manages, and revokes certificates that identify users for subsequent authentication using public key technology. The certificate server will also support installation and configuration of different certificate issuance policies and multiple certificate signature algorithms. Microsoft's CA effort includes a focus on code-signing that provides "shrink wrap" for the Internet. It identifies the publisher of an application and ensures that the application has not been altered before or during downloading. Code signing is supported in Microsoft Internet Explorer 3.0.

Netscape Communications

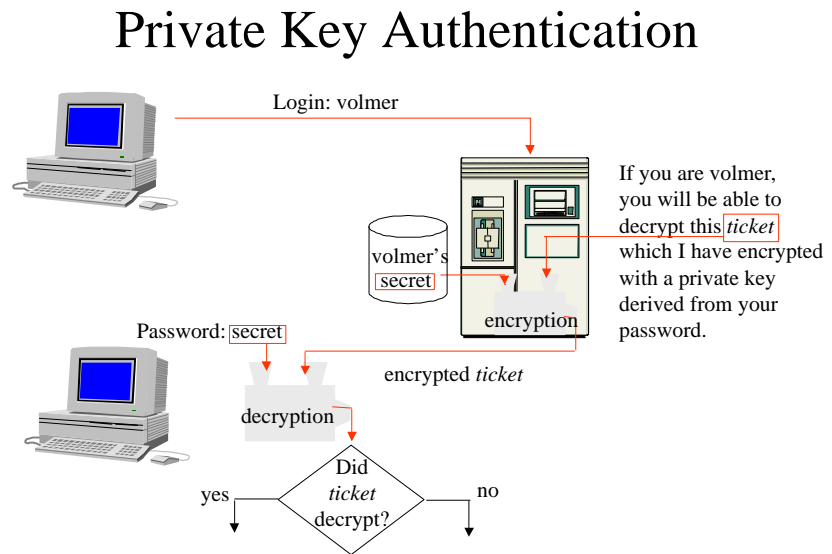
Netscape's Certificate Server is designed for a range of security applications and to support elements of electronic commerce. The server is priced at \$1,000. The Netscape Certificate Server is targeted primarily at the self-certifying marketplace where certificates are used for a range of intranet and Internet applications including secure messaging, legal and financial document management, secure single-user sign on to multiple servers using certificates instead of difficult-to-maintain unique user ID and passwords. It might also be used for cross certifying between closely aligned trading partners.

Application Issues

Some unresolved issues have been identified in the use of digital signature in applications. These issues are discussed in the following paragraphs.

- **Database Access**—The linkage between databases and certificate issuing and maintenance systems has been identified as a research issue.

- **Web Browsers**—Each application stores keying information privately, so that keys acquired by one application, such as a browser, cannot be used with another application, such as a database access program. On Microsoft platforms, since a common cryptographic service is provided to applications, private key sharing can be achieved in principle. On Unix, no such basic service is provided.



- **Domain Naming System (DNS)**—Client-generated information did not need to be kept in DNS before, but now client-generated public keys will need to be maintained.
- **Directory Services**—A directory service is a combination of locally maintained data, such as e-mail addresses, and personnel data, such as employee ID and telephone numbers. Directory updates are under the control of the one party that maintains the directory. Public key certificates form a third source of data. Some certificate authority software assumes complete control over directory updates, contrary to the directory service model.
- **Notary Service**—A digital signature by a third party with a time stamp can provide an equivalent of a notary service. The PKI infrastructure used and the digital signature formats dictated must be interoperable and agreed upon by other parties. Some potential uses of third party time stamping are ensuring legality of electronic records, establishing research records for patent purposes, and ensuring nonrepudiation for electronic commerce transactions. Digital notary services has been identified as a research issue for DOE.
- **Video Teleconferencing**—Multicast security, the protocols and the cryptography used, has been identified as a research issue within DOE. Public key technologies could be used to perform key exchange for privacy of traffic, authentication to limit group membership, and access control to group collaborative documents.
- **Software Bus**—A software bus allows applications to be glued together by providing and defining a common means of invoking operations and passing data between applications. Authentication and security in software bus services are still in the proposal stage.

Chapter 4. Digital Signature Standards

Implementation of the digital signature function will require Departmentwide interoperability as well as interface with vendors. To accomplish this, standards guidance is required to assist in reaching the necessary level of interoperability. Uncoordinated efforts can be duplicative, costly, and incompatible. Standards applicable to digital signature are to be used by anyone involved in the acquisition, development, implementation, maintenance, or management of applications using digital signature.

Digital signature standards being proposed for adoption or retirement are to be submitted to the Information Technology Standards Program Manager in the Office of the Chief Information Officer. The Standards Program Manager then initiates the Departmentwide process for adoption or retirement of the proposed standards. For further guidance on standards adoption or retirement, refer to the following documents: *Department of Energy Standards Adoption and Retirement Process* and the *Department of Energy Information Architecture Profile of Adopted Standards*. These document can be found online at the following URL: <http://www-it.hr.doe.gov/standards/>.

The standards identified by the DOE Digital Signature Working Group represent guidance for achieving digital signature interoperability within the DOE community. While these standards are not mandatory, it is recommended that they be incorporated into DOE digital signature implementations. Most of these standards have been through the DOE IT Standards Adoption and Retirement Process and are part of the DOE Profile of Adopted IT Standards and the corresponding Standards Repository. Abstracts of these standards can be found on the DOE Information Architecture Standards Home Page (see above for website address).

Federal Standards

There are several Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST) that apply to various aspects of digital signature. Discussions of these standards follow.

FIPS PUB 46-2 - Data Encryption Standard (DES) is the standard for the encryption of the private key and specifies a FIPS-approved cryptographic algorithm required by **FIPS PUB 140-1** (See below). This FIPS provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. DES was first approved in 1977 and was reaffirmed by the Secretary of Commerce in 1993, to be reviewed again in December 1998. In 1993 the following statement was included in the standard: “*At the next review (1998), the algorithm specified in this standard will be over twenty years old. NIST will consider alternatives which offer a higher level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review.*”

NIST is in the process of developing an Advanced Encryption Standard (AES), a very strong symmetric block cipher for government and commercial use in the next century. AES will be more efficient, more secure, publicly defined and evaluated, and will feature a worldwide royalty fee.

FIPS PUB 140-1 - Security Requirements for Cryptographic Modules is a general standard that, among other things, sets out requirements for cryptographic algorithms. This standard is the only one mentioned by the New Mexico state legislature concerning digital signature. Conformance to FIPS 140-1 is required for Federal Agencies if it is determined that cryptography is necessary for protecting unclassified information or when designing, acquiring, and implementing cryptographic-based security systems. Several vendors of digital signature software have sought and received FIPS 140-1 accreditation. This accreditation is done through testing by one of three testing laboratories:

- CEAL: A CygnaCom Solutions Laboratory in McLean VA
- DOMUS Software Limited IT Security Laboratory in Ottawa, Ontario
- InfoGard Laboratories in San Luis Obispo, CA

The following vendors are among those that have achieved FIPS 140-1 accreditation for their products:

- Entrust Technologies
- Netscape Communications Corp.
- Motorola, Inc. Land Mobile Products Sector
- SPYRUS, Inc. (Fortezza Crypto Card)
- IRE, Inc. (SafeNet line of TCP/IP based VPN [gateway] encryptors)
- Cylink Corporation
- Mykotronx, Inc. (Fortezza Crypto Card)
- Chrysalis-ITS (Luna token, LunaCA)

FIPS PUB 171 - Key Management Using ANSI X9.17 specifies a particular selection of options for the automated distribution of keying material by the Federal Government when using the protocols of ANSI X9.17-1985. ANSI X9.17-1985 protocols define procedures for the manual and automated management of keying materials and the use of DES to provide key management for a variety of operational environments.

FIPS PUB 180-1 - Secure Hash Standard (SHS) is the standard for the hash function. SHS specifies a Secure Hash Algorithm (SHA-1) for computing a condensed representation of a message or a data file.

FIPS PUB 186 - Digital Signature Standard (DSS) specifies a Digital Signature Algorithm (DSA) for the public key portion of a digital signature. DSS was selected by NIST, in cooperation with the National Security Agency, to be the digital authentication standard of the U.S. Government. This standard shall be used in designing and implementing public key-based signature systems that Federal departments and agencies operate or that are operated for them under contract. Adoption and use of this standard are available to private and commercial organizations. Currently there are few companies that provide products that meet the specifications of FIPS 186, and those that do are for very limited applications. NIST issued in the Federal Register May 13, 1997, a request for comment for the revision of FIPS 186 in order to utilize commercial off-the-shelf software for digital signatures. The comment period ended August 11, 1997. According to NIST, the reviewing body is now waiting for the Banking Standards Committee to adopt the ANSI X9 standards regarding the elliptical curve and RSA-based algorithm for financial services. When this occurs, within approximately six months, NIST will then incorporate by reference these standards into FIPS-186, allowing the use of these alternate technologies.

FIPS PUB 196 - Entity Authentication Using Public Key Cryptography specifies two challenge-response protocols by which entities may authenticate their identities to one another. Depending on which protocol is implemented, either one or both entities involved may be authenticated. The defined protocols are derived from an international standard for entity authentication based on public key cryptography. The authentication protocols described in the standards may be implemented in software, firmware, hardware, or any combination thereof.

Institute of Electrical and Electronics Engineers (IEEE) Standards

Several IEEE standards provide interoperability options for digital signature technology.

IEEE 1003.1e Portable Operating System Interface (POSIX)–Security Extensions specifies security considerations with respect to data encryption mechanisms, access control, reliability control, systems logging, fault tolerance, and audit facilities. This standard defines security capability necessary to secure kernel operations.

IEEE 1003.2c Portable Operating System Interface (POSIX)–Security Extensions defines the security interface for use by users and batch processing scripts that seek access to secure systems.

IEEE 1003.22 Guide to the POSIX Open Systems Environment–A Security Framework provides a focus for definition and placement of security services around which implementations and API standards activities may coordinate. The standard specifies the types of APIs required to

support the security services defined in the framework; identifies existing implementations and their relative maturity as potential base specifications for API standards and those areas with no existing or immature industry practice that require development efforts; provides a tool to help integrators of secure systems understand and structure security services within a distributed system; and provides a framework for structuring security within distributed systems based on ECMA-Security in Open Systems.

IEEE 1003.6 Security Interface Standards for POSIX provides changes and additions for security-related functional requirements and system interfaces in the areas of accountability, extended discretionary access control, mandatory access control, security information labeling, and fine-grained capabilities. The standard provides developers with the option of using interfaces to implement portable applications with security features, and to determine how to apply security policies relating to accountability, discretionary access control, mandatory access control, and capabilities (privilege) to existing interfaces.

International Standards

ISO/IEC 9796:1991 Information Technology–Security Techniques–digital signature scheme giving message recovery and **ISO/IEC 9796-2: 1997 Information Technology–Security Techniques–digital signature schemes giving message recovery–Part 2: mechanism using a hash function** deal with encryption and authentication.

Although there have been several proposed formats for public key certificates, most certificates available today are based on an international standard (ITU-T X.509 version 3). **Revision to ITU-T Recommendation X.509, (Also specified in ANSI X9.55-1995[X9.55] and IETF Internet Public Key Infrastructure working document [PKIX1])** defines a certificate structure that includes several optional extensions. The X.509 version 3 certificate includes the following: Version, Serial Number, Issuer Signature Algorithm, Issuer Distinguished Name, Validity Period, Subject Distinguished Name, Subject Public Key Information, Issuer Unique Identifier (optional), Subject Unique Identifier (optional), Extensions (optional), and Issuer's Signature (authenticating all the above fields). The use of X.509v3 certificates is important because it provides interoperability between PKI components.

Emerging Standards

Several standards are being proposed by consortia, working groups of standards bodies or task forces. Discussions of these standards follow.

X.500–Information Technology–Open Systems Interconnection–The Directory: Overview of concepts, models, and services is a family of standards that uses a distributed approach to a global directory service. Local information for an organization is maintained locally in one or more so-called directory system agendas. X.500 offers the following features: decentralized

maintenance, powerful searching capabilities, single global namespace, and structured information framework.

Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services. It runs directly over Transmission Control Protocol (TCP), and can be used to access a standalone LDAP directory service or to access a directory service that is back-ended by X.500. The LDAP Standard defines: a network protocol for accessing information in the directory, an information model defining the form and character of the information, a namespace defining how information is referenced and organized, and an emerging distributed operation model defining how data may be distributed and referenced (v3).

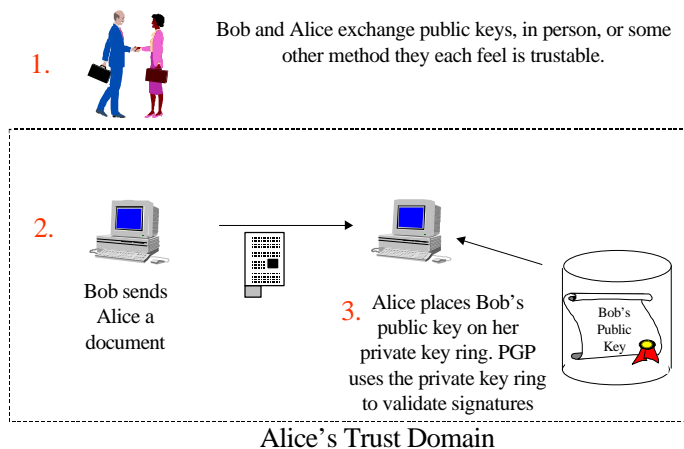
Minimum Interoperability Specification for PKI Components (MISPC), Version 1, June 5, 1997, supports interoperability for a large scale PKI that issues, revokes, and manages digital signature public key certificates, to allow the use of those signatures to replace handwritten signatures in government services, commerce, and legal proceedings, and to allow distant parties, who have no previous relationship, to reliably authenticate each other and conduct business. The MISPC addresses: public key certificate generation, renewal, and revocation; signature generation and verification; and certificate and certification path validation. MISPC is a NIST Cooperative Research and Development Agreement (CRADA)..

MISPC provides a basis for interoperation between PKI components from different vendors. This specification will be available to companies interested in offering interoperable PKI components, to Federal agencies developing procurement specifications, and to other interested parties. It will be the basis for a NIST reference implementation and an initial root Certification Authority for the Federal PKI.

Pretty Good Privacy (PGP) is a high-security cryptographic software application that allows people to exchange messages with both privacy and authentication. Privacy means that only those

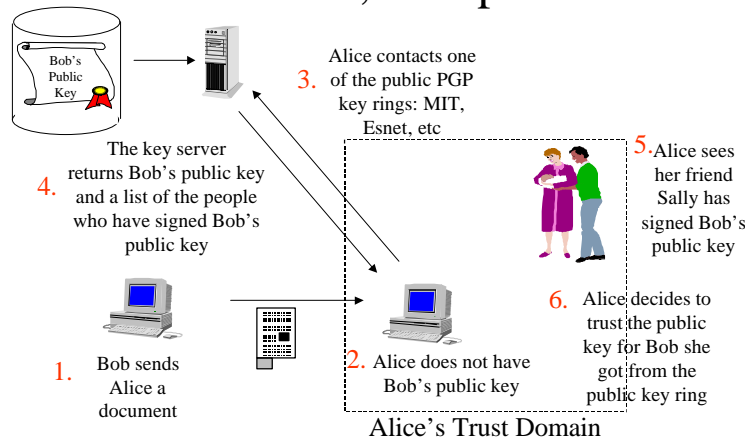
intended to receive a message can read it. By providing the ability to encrypt messages, PGP provides protection against anyone eavesdropping on the network. Even if a packet is intercepted, it will be unreadable to the snooper. Authentication ensures that a message from a particular person originated from that person only, and that the message has not been altered.

PGP Mechanics, Simple Case



The MIME Object Security Services (MOSS) protocol,

PGP Mechanics, Complex Case



currently in draft form within the Internet Engineering Task Force (IETF) Network Working Group, uses the multiparty/signed and multiparty/encrypted framework to apply digital signature and encryption services to MIME objects. The services are offered through the use of end-to-end cryptography between an originator and a recipient at the application layer. Asymmetric (public key) cryptography is used in support of the digital signature service and encryption key management. Symmetric (secret key) cryptography is used in

support of the encryption service. The procedures are intended to be compatible with a wide range of public key management approaches, including both ad hoc and certificate-based schemes. Mechanisms are provided to support many public key management approaches.

The issue of secure World Wide Web transactions has resulted in two competing proposals: **Secure Sockets Layer (SSL)** and **Secure Hypertext Transfer Protocol (S-HTTP)**. So far neither has been determined to be the winner. Both could be enabling technologies for using WWW technology for sensitive information and secure transactions where data privacy, data integrity, authentication, and nonrepudiation are concerns.

Secure Sockets Layer (SSL) is an open protocol for securing data communications across computer networks. Incorporating RSA data security technology, SSL provides a straightforward method for adding strong security to existing applications and network infrastructures. SSL is application protocol independent and provides encryption, which creates a secured channel to prevent others from tapping into the network; authentication, which uses certificates and digital signatures to verify the identity of parties in information exchanges and transactions; and message integrity, which ensures that messages cannot be altered en route.

Secure Hypertext Transfer Protocol (S-HTTP) provides secure communication mechanisms between an HTTP client-server pair in order to enable spontaneous commercial transactions for a wide range of applications. The design intent is to provide a flexible protocol that supports multiple orthogonal operation modes, key management mechanisms, trust models, cryptographic algorithms, and encapsulation formats through option negotiation between parties for each transaction.

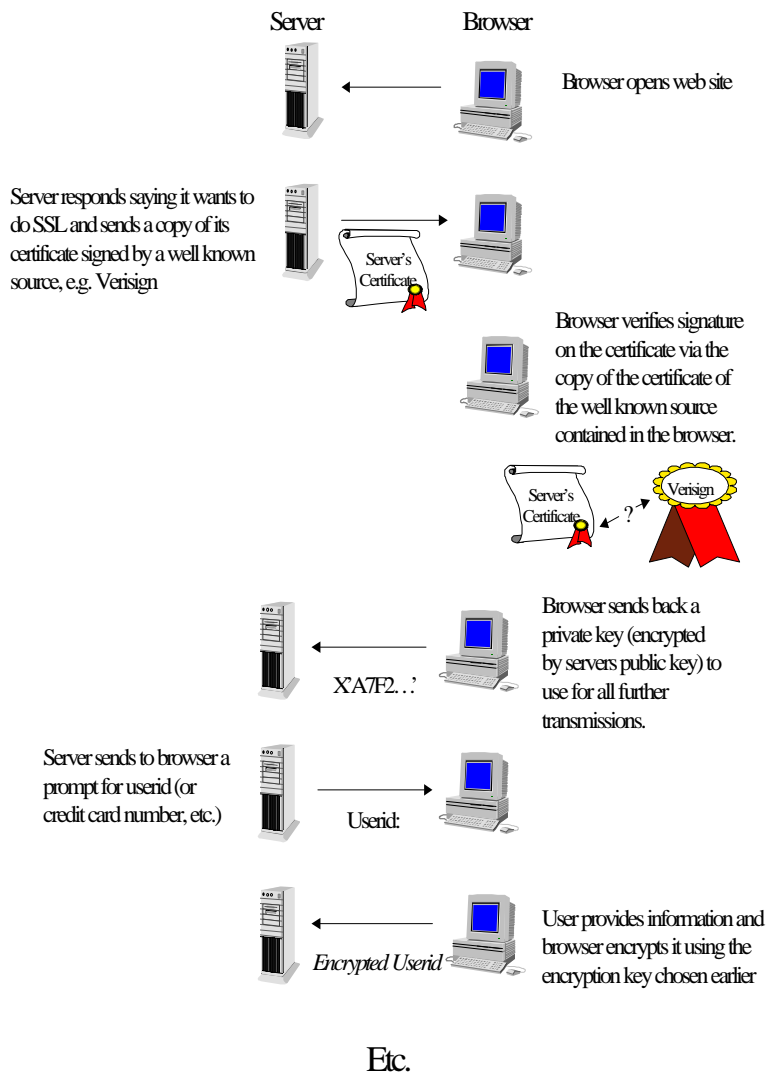
RSA Public Key Cryptography is a public-key crypto system for both encryption and authentication. RSA supplements DES (or any other fast bulk encryption cipher) and is used

together with DES in a secure communications environment. For encrypting messages, RSA and DES are usually combined as follows: first the message is encrypted with a random DES key, and then, before being sent over an insecure communications channel, the DES key is encrypted with RSA. Together, the DES-encrypted message and the RSA-encrypted DES key are sent. This protocol is known as an RSA digital envelope.

Kerberos, DCE-SS 1.1 Generic Security Service API (GSS API) is a distributed

authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal. Kerberos optionally provides confidentiality and integrity for data sent between the client and server. Version 5 of Kerberos is considered to be the standard.

SSL Protocol



The Open Software Foundation's Distributed Computing Environment (DCE) Security Service component is based upon Kerberos Version 5. In order to support applications that need to be portable across a variety of underlying security mechanisms, a "Generic Security Service API" (or GSS API [Internet RFC 1508]) was designed; it gives access to a common core of security services expected to be provided by several mechanisms. As an accepted standard for distributed authentication and authorization, Kerberos is a fundamental requirement for a robust distributed computing environment.

Chapter 5. Records Management

Records managers serving DOE programs and missions face a variety of challenges and opportunities in their attempts to deliver quality records management services in a complex computing technology environment. As the use of digital signature technology becomes more commonplace in DOE business processes, records managers will be presented many new obstacles to overcome in their attempt to serve their customers. These obstacles will arise from changing procedural expectations, new business practices, evolving computing technologies, and the automation of previously manual processes.

Records management functions in the Federal sector are largely performed with paper records. Many of the issues of using digital signature for records management are similar to issues for using electronic versus paper records without digital signature. Including a records management chapter in this document does not mean that extensive use of digital signature for records is contemplated in the near future. However, any current application of digital signature must address records management issues.

When contemplating extensive use of digital signature for records, a DOE enterprisewide solution should be encouraged, based on requirements commonality and application standardization. A digital signature system needs to be a uniform system for archiving electronic records or documents, address evidentiary issues, and support the belief that electronic documents should be retrievable for many years without concerns regarding unauthorized document modification.

There are several records management issues with regard to digital signature. These are addressed in the following sections.

Storage and Retrieval Problems

Electronic media do not readily store records in a manner supportive of long-term document storage. In addition, there are no clear organizational guidelines on who must budget for the eventual data conversion that must occur to keep stored electronic records retrievable over a considerable period of time—Records Management or the originating organization?

The systems and file formats in which records are stored will become obsolete, and moving data to newer computers will result in losing the ability to read the original data or validate attached signatures, unless the same digital signature software can be implemented in the new computing environment. How both signature objects and viable software can be preserved across computing architectures and the life cycle of records has not been addressed in most discussions of the implementation of digital signature technology. It is very important to create and maintain an inextricable link between the digital signature and the record throughout its disposition cycle to address concerns about information authenticity.

Paperless Versus Paper Records

It should be clear as to whose responsibility it is to verify that the electronic records adequately document transactions and functions and that the paper copies of these records sent to the record center may be safely destroyed as redundant information. It should be specifically stated that this is the responsibility of Records Management or the owning organization.

One of the primary records concerns at the DOE sites with regard to paperless computer systems that use digital signatures is that there is little overlap between procedures for managing paper records and the procedures that apply to information in electronic systems. There is often an expectation that a paper counterpart of an electronic record should be producible on demand, even if the document was not originally printed during its active life. It is also desirable to be able to attest that a paper document was printed at some particular time from a computer system in a manner similar to what might be an electronic counterpart of a notary.

Consideration of whether electronic documents using digital signatures can be used to replace sending the record copy to hard copy records centers is premature at this time. The Savannah River Site has plans to test record authentication using digital signature as part of its Documentum electronic document management system. Such records can be retrieved and certified as not altered through digital signature validation. However, most sites have not implemented this advanced level of document management and are still very involved in the integration of electronic and hard copy business processes. Password authentication/e-mail approval is being used and is (slowly) replacing hard copy documents for many documents that may have formerly been signed.

The issue of managing, in an integrated manner, the digitally signed electronic documents that are stored in a different location from the related paper documents must be addressed. Scanning has become very cost-effective for the Savannah River Site where a single meta-data database that stores index information for both paper and electronic holdings is used. At other sites, consideration is being given to using an electronic records system that allows for location cross-referencing of documents. For example, the system could allow one to enter location of the record with a cross-reference to either the paper or electronic record. However, this level of integrated electronic and paper document tracking is beyond the capabilities of most present systems. Lockheed Martin Energy Systems is using the Electronic Information Content Management System (EICMS) to address this issue.

A good solution is to concentrate on properly designating and scheduling the record copy. Since most paper documents are now produced by computer systems, they will increasingly be seen as supportive information that is not really record copy, and therefore no hard copy version should be designated/scheduled as record copy.

Who Signed What?

It is important to be able to determine who signed which version of a document at which point in the business process and which items on a form or document were signed by specific individuals. Due to the manner in which digital signatures are applied to electronic documents, it is often difficult to determine what parts of a document were signed by particular individuals. One digital signature or a set of signatures that exists as an “envelope” around a complete document could be confusing in establishing precise responsibilities for the authorization of portions of an electronic record.

Creation of New Records

Because of the perceived importance of electronic documents signed with digital signatures, it is important that they are associated with records series and, consequently, retention schedules so that they will be retrievable throughout their life cycle. This will also be required to assure that records are disposed of at proper intervals. It is desirable to have some records management controls designed into the document management aspects of the digital signature computer systems.

It will be important to assure that the definition of a record is followed closely to prevent creating more electronic records than necessary, as electronic records may not be “cheap to keep.” One category of new records that will be created through the use of digital signature is certificates. If a digitally signed document is archived, there will be a need to also archive the associated public key certificate. There will be many issues to address concerning how and with what other information this archiving will occur.

National Archives and Records Administration (NARA) Issues

Issues about transmitting electronic records that are digitally signed to the National Archives and Records Administration (NARA) must be addressed. Two of the issues are media and computing infrastructure. NARA will need to accept electronic documents with attached signatures on a long term electronic storage media, such as CD-ROM. NARA will also have to approve the transfer and accept the digital signature. At the present time, NARA is only interested in archiving documents, not digital signature storage and retrieval.

In addition, an interagency PKI might be needed to allow the direct transfer of such files to NARA. Software and interfaces that would enable transferring records to NARA must be acquired or developed. Considerable concern exists about avoiding a separate system just for transmitting records to NARA. A clearly defined records migration strategy must be developed to specify responsibilities for maintaining records, once records are transferred to NARA in a NARA acceptable format. Most sites do not want to maintain duplicate copies of records transferred to NARA.

Recommendations for Records Managers

Records Managers deliver information management services to organizations and individuals.

However, these Managers are rarely the initiators of computing technology changes within organizations. Records management departments usually attempt to follow the technology changes initiated by their customers and to build computing systems that integrate smoothly within the computing architectures used by their customers.

However, Records Managers will need to be constantly reaching out to their customers, including their own management, to build interest, support, and assistance in meeting these new challenges. The organizations that they support must be ready to include Records Managers in strategic planning meetings and technology implementation projects so that records management issues can be addressed. This need for strong interaction between Records Managers and their customers permeates the issues presented in this chapter.

One significant solution is that records management requirements need to be developed to be added to computer system technical requirements. These requirements would identify the archiving, evidentiary, and validation objectives that must be met by any electronic record/digital signature system. These records management requirements need to be built with significant input from auditors and attorneys, who may in the near future be in the position of challenging an electronic record keeping system. This will also become important as sites begin to implement software, such as SAP, that may question the concept of what information is really a database record. Once these criteria are developed; they should be used in conjunction with technical criteria to run pilots at selected DOE sites.

Records Retention Periods

The General Records Schedules (GRS) and Department of Energy Records Schedule (DOERS) provide the retention period of certain records common to most of the DOE complex. It is hoped that the following list will assist users in deciding what records might be considered acceptable for the use of digital signatures in light of current records retention requirements.

- Payroll correspondence (GRS 2.24)–Destroy after 2 years
- Records of reports of routine safety inspections (DOERS 1.1.c)–Destroy after 1 year
- Routine procurement files (less than \$25,000 and less than \$2,000 for construction projects) (GRS 3.3.a)–Destroy 3 years after final payment
- Routine procurement files including correspondence (over \$25,000, and any construction projects greater than \$2,000) (GRS 3.3.a)–Destroy 6 years and 3 months after final payment
- Correspondence files relating to facility safety program (DOERS 1.1.b)–Destroy when 10 years old
- Researcher's biology notebooks (DOERS 1.10.a)

S Of exceptional value—Permanent (offer to NARA in 25 years)
S Not of exceptional value—Destroy after 15 years

- Patent application case files (DOERS 7.2)—Destroy 25 years after date of last action
- Facility design and construction planning (DOERS 14.1.c)—Retain until dismantlement of facility
- Unscheduled records (includes waste characterization)—Permanent (offer to records, research, and development files) (offer to NARA in 25 years)

Chapter 6. Legal Considerations

The technology upon which digital signatures is based is neither fully developed nor widely implemented. Since digital signatures are not widely used, the law presently is relatively undeveloped, but will likely develop rapidly once digital signatures are widely deployed. Given the recent emergence of digital signature technology and the fact that the supporting institutional infrastructure and processes are far from fully in place, the law of digital signatures is relatively undeveloped, with few judicial decisions having been issued.

The Digital Signature Working Group has identified certain risks and potential liabilities as well as responsibilities that should be considered when planning the use of digital signatures. Program officials are encouraged to involve their legal staff early on in any digital signature initiatives. Providing them with a copy of this report will be helpful since it contains useful background and references and could serve to expedite responses to legal questions.

Persons needing to address or resolve legal issues associated with digital signatures should review the American Bar Association *Digital Signature Guidelines*, published in 1996, which provides a comprehensive framework to assist in the drafting and interpretation of digital signature legislation. This publication has a tutorial to educate readers on how digital signature technology works and a brief overview of signatures and the law in general. The text of the guideline provides general statements of principle, which is intended as a common framework of unifying principles and comments on these general principles, for the use in drafting digital signature statutes. Such a review will provide a good general perspective regarding the use of digital signatures and valuable insight concerning the identification and allocation of specific risks among all parties involved.

The American Bar Association *Digital Signatures Guidelines Tutorial* says that in order to achieve the basic purposes of signatures, a signature must have the following attributes:

- **Signer authentication**—A signature should indicate who signed a document, message, or record, and a signature should be difficult for another person to produce without authorization.
- **Document authentication**—A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.
- **Affirmative act**—The affixing of the signature should be an affirmative act that serves the ceremonial and approval functions of a traditional signature and establishes the sense of having legally consummated a transaction.
- **Efficiency**—Optimally, a signature and its creation and verification processes should provide the greatest possible assurance of both signer authenticity and document authenticity, with the least possible expenditure of resources.

Digital signature technology generally surpasses paper technology in all these attributes. The likelihood of malfunction or tampering in a digital signature cryptosystem designed and implemented according to Federal/industry standards is extremely remote and is far less than the risk of undetected forgery or alteration on paper or of using less secure electronic signature techniques.

Legal issues involving digital signatures can be divided into three categories:

- Evidentiary issues
- Liability/responsibility issues
- Enforceability/nonrepudiation issues

A discussion of evidentiary issues follows. Other issues are not discussed in this issuance of the document because of a lack of definitive answers.

Evidentiary Issues

Currently, the use of digital signature technology is most widespread in the area of commerce. The courts have not yet dealt with records maintained in digitized form and may not even comment for several years, if history is any guide. It took several hundred years for the courts to accept paper records into evidence, approximately 40 years to accept microfilm, and approximately 10 years to accept computer-generated records. Similarly, the acceptance of this new technology will depend upon the comfort level of the judges and administrators.

A study conducted by Martin Marietta Energy Systems to develop a Prototype Electronic Records Management System (PERMS) for the U.S. Army Information System Command, under contract to the DOE in Oak Ridge, Tennessee, was initiated to test the concept of combining an electronic document management system and a digital signature system into an overall system that could withstand judicial scrutiny. The electronic signature capability was designed to meet four requirements: not forgeable, authenticatable, unalterable, and not reusable.

Several recommendations were made during the PERMS research project to assure compliance with legal statutes. Providing unrestricted access to appropriate users, good system security, adequate data interchange formats, and means for the appropriate disposition of documents answered many of NARA's concerns. Steps to assure the legal admissibility of documents as court evidence include documentation of business processes and system security, identification of records media life cycle, and coordination of issues with records management staff and legal counsel.

It was recommended that a written agreement between authorized system users and system managers be executed that specifies the jurisdiction under whose laws the agreement is to be

governed and the forum of litigation of disputes, as well as a stipulation that the parties will be bound by their digital signatures. Although such efforts will not preclude all disputes, they will serve to support acceptance of the overall validity of digital signatures pending legal and/or regulatory interpretation.

Current legal attitudes toward computer records in general are reflected in both statutes and case law. The **Uniform Rules of Evidence** provides the basis for admitting all types of records, including computer records, into evidence. The rules specifically refer to computer records in **Rule 803(6)** by using the term “data compilation.” Under **Federal Rule of Evidence 803(8)**, however, if the only record is electronic, procedures should be established and followed so that:

- The date of the record can be determined
- The date of any alterations will be automatically recorded by the system
- It will be evident that the document was authorized to be issued (“signed”).

The **Federal Rules of Evidence Rule 1001(1)** states, “‘writings’ and ‘recordings’ consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.” Nothing in this definition precludes the use of encryption technology. Similarly, when defining an original, **Rule 1001(3)** states, “an ‘original’ of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it.... If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original’.”

State Legislation for Electronic and Digital Signatures

Currently there are 40 states that have either considered or enacted electronic authentication laws. Of these, 23 states have enacted some type of limited law statute, and 10 states have enacted a general statute. The majority of the states have enacted electronic signature laws, but only a few have enacted digital signature laws. While the terms “electronic signature” and “digital signature” are often used interchangeably, the definitions are different. To simplify, a “digital signature” uses an encryption methodology, while an electronic signature uses letters, characters, or symbols.

Most of the states’ digital and electronic signature initiatives fall into three categories:

- **Prescriptive**—Statutes delineate specific PKI schemes for digital signatures and have a general applicability. Utah is an example of a state using this model.

- **Criteria-based**—Statutes recognize the authentication of digital or electronic signatures, provided the signatures satisfy certain criteria of reliability and security. California provides the leading model of a criteria-based approach.
- **Signature enabling**—Statutes recognize electronic signatures and documents in a manner that is parallel to traditional signature and writing laws. These are technology-neutral as they adopt no specific technological approach or criteria. Massachusetts is the leading state using this model.

For a more in-depth analysis of the types of models and the statutes enacted by each state, see the site for Internet Law and Policy Forum at <http://www.ilpf.org/digsig/digsig.htm>. The following states have enacted digital signature technology statutes: Florida, Indiana, Minnesota, Mississippi, New Hampshire, New Mexico, Oregon, Utah, and Washington.

Federal Agencies

The Food and Drug Administration (FDA) issued regulations (21 CFR part 11) that provide criteria for acceptance by the FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. The effective date of these regulations was August 20, 1997. The rule sets forth controls for document encryption and the use of appropriate digital signature standards to ensure record authenticity, integrity, and confidentiality.

Federal Legislation

Currently, there are no Federal statutes about digital signature. However, it is anticipated that there will be Federal legislation on the topic. Several bills that have been proposed are discussed in the following paragraphs. Information on the status of these bills is published on the World Wide Web at <http://www.congress.gov/>

Senate Bill 909: Secure Public Networks Act, introduced in June 1997 by Senator McCain (commonly referred to as the McCain/Kerry bill), mandates the use of key recovery encryption in any federally supported network, including universities. The bill also states that law enforcement would require only a subpoena to access private keys, whereas current Federal regulations require a court order. This bill was passed by the Senate Commerce Committee in June 1997.

H.R. Bill 695: Security and Freedom Through Encryption (SAFE), introduced in February 1997 by Representative Goodlatte, originally allowed for the exportation of encryption technology and sought to ban Federally mandated key recovery. Recent amendments made by legislators have instead "marked up" the bill, or amended it at the committee level, to reflect the wishes of the Federal Bureau of Investigation (FBI) (see below) and other law enforcement agencies that want "wiretap" access to all encrypted e-mail and other digital files. The amendment, passed 45 to 1 on September 9, 1997, by the House National Security Committee,

radically changed the SAFE bill by reaffirming government export regulations on cryptography. The amendment would return control of all encryption exports to the President, who would set a "maximum level" for exportable encryption once a year. After a one-time review, all products that did not exceed that limit would be allowed to be exported.

The FBI in September 1997 began circulating new draft encryption legislation that would impose mandatory key recovery. This legislation would impose full domestic controls on the manufacture and use of encryption. In addition, it would require all network service providers that offer encryption products or services to their customers to ensure that all messages using such encryption can be immediately decrypted without the knowledge of the customer. This would apply to telephone companies and to online service providers such as America Online and Prodigy.

H.R. 2937, Electronic Financial Services Efficiency Act of 1997, provides that in any written communication with any Federal agency or instrumentality, or any U.S. court, which calls for a signature, any party to the communication may affix a digital signature with a certificate issued by a trusted third party. Also, all forms of electronic communication that comport with the standards prescribed by this Act shall have standing equal to paper-based written signatures with respect to Federal agencies, courts, and instrumentalities, as well as in general.

The bill also establishes the National Association of Certification Authorities, of which any person wishing to provide electronic authentication services shall be a registered member. It prescribes membership guidelines and requires the Association to establish the Electronic Authentication Standards Review Committee, with rulemaking and enforcement powers, which shall: establish, develop, and refine criteria for application to the emerging electronic authentication industry; and report biannually to the Secretary of the Treasury. This legislation is in committee.

H.R. 2991, Electronic Commerce Enhancement Act of 1997, is in committee. It directs the Assistant Secretary for Communications and Information (the head of the National Telecommunications and Information Administration) of the Department of Commerce to conduct an ongoing study of and report to specified committees concerning the enhancement of electronic commerce due to the use of digital signatures pursuant to this Act. It directs the Director of the Office of Management and Budget to establish a method for each Federal agency to make its forms available electronically. It provides for making payments electronically pursuant to such forms. It sets forth provisions concerning guidelines and standards for digital signatures and certificates. It permits employers to store forms electronically if such forms are submitted electronically.

Choice of Law

Concerns have been expressed over which law, state or Federal, would control an electronic record. Many contracts state the choice of law, Federal or state, to be used in contract disputes.

Chapter 7. Next Steps

The Digital Signature Working Group (DISIWG) will continue to function as a focal point for collaboration and cooperation and sharing of knowledge and experience in the area of digital signature. This first issuance of digital signature guidance and considerations serves as an introduction to the topic. Periodic updates are expected, as DISIWG members have more experiences to share, as the technology matures and is more widely used, and as legislation is enacted.

One of the current pilot applications of digital signature is the Chief Financial Officer (CFO) application with Travel Manager. The CFO is building on a framework established by the National Institute of Standards and Technology (NIST) and is using a solution proposed by CygnaCom Solutions. The Assistant Secretary for Energy Efficiency and Renewable Energy (EE) is using the same solution for a procurement application.

Sandia National Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Kansas City (Allied Signal), and the Assistant Secretary for Information Management in Germantown are all cross-certified. All locations are using Entrust software, and are experiencing no significant problems. The total user community numbers around 1000. Savannah River, Oak Ridge, and Pacific Northwest National Laboratory are in the process of joining this community. The Headquarters location is acting as the certificate authority for all DOE Federal staff.

Chapter 9 of the Telecommunications Security Manual, DOE M 200.1-1, defines the roles, requirements, and responsibilities for establishing and maintaining and the documentation necessary to ensure that all certificates are managed in a manner that maintains the overall trust required to support a viable PKI. This chapter is being reviewed and enhanced through the DOE Directives process. When the process is complete, Chapter 9 should serve as a broadly based policy for PKI at DOE.

A possible direction for DISIWG is the shepherding of a lightweight PKI infrastructure that deals with broad issues, such as what fields should be included in an X.500 directory or how to locate, establish, and authenticate the identity of a certificate authority. Ensuring that the current CA is valid and correct is an outstanding problem in the PKI arena. A common operating policy is important, too. A CA must work in a secure environment to protect private keys. When DOE acknowledges a site's CA, there should be a contractual arrangement or common policy agreement with sites that the CAs are operating in a secure manner.

Gartner Group, in a Strategic Analysis Report published in August 1997, predicted the following.

- By 1999, the widespread deployment of local Certificate Authorities (CAs) will cause the ad hoc creation of hierarchical CA systems, resulting in a critical mass for widespread use of digital identification.
- The U.S. Postal Service's CA will dominate public-service CA applications involving consumers and inter-agency applications by the year 2002, but other CA credentials will also be accepted for public agency relationships with corporate entities.
- There will be no Federal legislation or standard regulations that will clearly define the duties and legal liabilities of third-party CAs by 1999.
- Biometrics will emerge in the 2002 time frame as a cost effective way to bind an individual user to a specific action or transaction or to grant access to resources and will be used in 20 percent of all authentication applications. Biometric techniques may be based on fingerprint scanning, retinal scanning, or keyboard ballistics (a technique based on measuring the rhythms of users as they enter passphrases).

Appendix A: References

References

Public Key Infrastructure



Telecommunications Security Manual, DOE M 200.1-1, Chapter 9

National Institute of Standards and Technology Computer Security Division, PKI Specifications to support the DOE Travel Manager Program, August 15, 1996 Available at <http://cio.doe.gov> and click on Computer Security

Standards

DOE IT standards repository and program-related information available at <http://www-it.hr.doe.gov/standards/>

Records Management

General Records Schedules (GRS). Available at <http://gopher.nara.gov:70/1/managers/federal/schedule>

Department of Energy Records Schedule (DOERS). Available at <http://ardor.nara.gov/doe/index.html>

Legal Considerations

American Bar Association Digital Signature Guidelines available at <http://www.abanet.org/scitech/ec/isc/dsg.html>

McBride, Baker & Coles, Summary of Electronic Commerce and Digital Signature Legislation, Available at http://www.mbc.com/ds_sum.html

Software Industry Issues: Digital Signatures, Available at <http://www.SoftwareIndustry.org/issues/1digsig.html#s1>

Applications

Gartner Group Strategic Analysis Report, August 6, 1997. *X.509 Certificate Authorities for Enterprise Security and Electronic Commerce*

Fred Avolio, Barbara Fox, Brian Schimpf, and Win Treese. Panel on security for WWW. In Symposium on Network and Distributed System Security. Internet Society, 1997

Christopher Allen. SSL discussion list FAQ, September 1996. Available at <http://www.consensus.com/security/ssl-talk-faq.html>

Richard Ankey. Introduction to cryptographic standards, 1996. Available at <http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/>

Apache HTTP server project home page. Available at <http://www.apache.org>

Microsoft Bay Area Research Center: Scalable servers project page (as of February 1997). Available at <http://research.microsoft.com/research/BARC/Scaleable/>

Kraig Brockschmidt. What OLE is really about, July 1996. Available at <http://www.microsoft.com/oledev/olecom/aboutole.htm>

Donald Eastlake, III and Charles Kaufman. RFC 2065: Domain name system security extensions. Technical report, CyberCash, Inc. and Iris Associates, 1997. Available at <ftp://ds.internic.net/> by clicking on rfc and then clicking on rfc2065.txt Extensions for signed DNS requests and responses and public-key resource records.

Entrust ISVs. Available at <http://www.entrust.com/> click on search and type ISV

S. Farrell, C. Adams, and W. Ford. Internet public-key infrastructure, part III: Certificate management protocols. Internet Draft, December 1996. Available at <ftp://ftp.ietf.cnri.reston.va.us/internet-drafts/> and click on draft-ietf-pkix-ipki3cmp-07.txt Internet Draft (PKIX Working Group).

Ian Foster, William Johnston, and the participants of the Workshop. Report for the second joint ER/DP computing-related security research requirements workshop, 1996. Available at http://www-itg.lbl.gov/DOE_Security_Research

Stephen Kent. Let a thousand (ten thousand?) CAs reign. In DIMACS Workshop on Trust Management in Networks. Center for Discrete Mathematics and Theoretical Computer Science, Oct 1996. Available at <http://dimacs.rutgers.edu/Workshops/Management/Kent.html> Steve Kent makes the argument that it has been difficult to establish a (general) certificate authority that satisfies the requirements of different user communities and application uses for a number of reasons: unwanted liability for the potential uses of certificates, different needs for authentication assurance when issuing, and naming. These issues are more understandable when the environment is sharply defined, hence the need for CAs for specific environments: user communities (such as an individual organization) and application uses (such as commerce or E-Mail).

Spectro-microscopy electronic notebook, 1997. Available at <http://www-itg.lbl.gov/~ssachs/notebook/project.html>

Lightweight Directory Access Protocol, 1996. Available at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>

Netscape home page. Available at <http://www.netscape.com>

NIST: Public key infrastructure program (as of February 1997). Available at <http://csrc.nist.gov/pki/>

Pekka Pessi. Secure multi-cast, 1995. Available at <http://www.tcm.hut.fi/Opinnot/Tik-110.501/1995/>

Tom Parker and Denis Pinkas. Extended generic security service APIs: XGSS-APIs access control and delegation extensions. Technical report, ICL and BULL, July 1996. Available at <ftp://ftp.ietf.org/internet-drafts/> and click on draft-ietf-cat-xgssapi-acc-cntrl-02.txt The extended GSS-API allows delegation of rights and association of additional security attributes other than identity. Example attributes include role, privileges, group, and restrictions.

Jaan Priisalu. A Frequently Asked Question list (FAQ) for alt.technology.smartcards, July 1995. Available at <http://www.ioc.ee/atsc/>

Matthew Richardson. PGP digital timestamping service, August 1996. Available at <http://www.itconsult.co.uk/stamper.htm>

RSA. PKCS #1, 1993. Available at <ftp://ftp.rsa.com/pub/pkcs/ascii/pkcs-1.asc> This describes an encoding of RSA private and public-keys, encryption and signature data formats.

RSA Laboratories, Inc. BSAFE 3.0 product description, 1996. Available at <http://www.rsa.com/rsa/products/index.html> BSAFE is a cryptographic API providing implementations of many public-key and secret-key algorithms. It is a basic building block present in many vendor products, such as the Netscape browser, the Java security library, Microsoft Windows.

S/MIME Editor. S/MIME message specification PKCS security services for MIME. Technical report, RSA, February 1996. Available at <http://www.rsa.com/pub/S-MIME/smimemsg.txt> Describes additions to MIME to support cryptographic signature and/or encryption services.

Walt Curtis (Entegrity Solutions). Information security in the enterprise. In RSA Data Security Conference, 1997.

Surety Technologies home page, 1996. Available at <http://www.surety.com/>

Walt Tuvell. Challenges concerning public-key in DCE, December 1996. Available at e-mail server, Send e-mail to dce-rfc-archive@osf.org with body consisting of two lines: "path your-email-address", "send rfc rfc98.0.ps".

M. Wahl, A Coulbeck, T Howes, and S Kille. Lightweight directory access protocol: Standard and pilot attribute definitions. Technical report, Critical Angle, Inc and Netscape and ISODE Consortium, October 1996. Available at [ftp://ftp.ietf.org/internet-drafts/](ftp://ftp.ietf.org/internet-drafts/draft-ietf-asid-ldapv3-attributes-03.txt) and click on draft-ietf-asid-ldapv3-attributes-03.txt

Oracle, Informix strengthen their commitments to CORBA. Available at <http://www.webweek.com/96Nov04/software/oracle.html>

XCert Software. Sentry: Access control list, 1996. Available at <http://www.xcert.com/software/sentry/acl/index.html> Using public-key certificates to authenticate end-users, you can specify ACL requirements for web servers.

XCert Software. Sentry: Certificate authority, 1996. Available at <http://www.xcert.com/software/sentry/ca/index.html> Provides LDAP server communicating over SSL.

XCert Software. Ssl-ldap, 1996. Available at <http://www.xcert.com/software/sentry/ca/index.html> Provides LDAP server communicating over SSL.

Tatu Ylonen. The SSH (Secure Shell) remote login protocol. Internet Draft, 1996., See also "SSH (Secure Shell) Remote Login Program" <http://www.cs.hut.fi/ssh/>